

WISTHLEBLOWER CHANNEL POLICY

AZKOYEN GROUP

- **Version control**

Version	Date	Author	Changes that have taken place
1.0	September 2019	Support Unit	Initial version
2.0	December 2021	Support Unit	Draft version: new Whistleblower Channel

- **Approvals**

Governing body	Entity	Date	Signature
Board of Directors	GRUPO AZKOYEN, S.A.	September 2019	

N.B. This version is in the process of being updated to assess the potential impact and changes arising from the implementation of the new whistleblower channel tool, as well as recent legislative changes which, in some cases, are pending transposition into the regulations of the European member states, which is expected to occur in Spain in 2022, and which could require changes in the wording of this policy.

1. Introduction to the Whistleblowing Channel	4
Subjective scope	4
2.1 Who should report through the Whistleblowing Channel?	4
2.2 Who can be reported through the Whistleblower Channel?	5
3. Objective scope	5
4. Means of receiving complaints How should you report?	6
5. Whistleblower protection measures	7
5.1 Prohibition of reprisals	7
5.2 Confidentiality about the identity of the whistleblower	7
5.3 Measures to deal with conflict of interest situations	8
6. Complaint handling procedure	8
6.1 Receipt of complaints	8
6.2 Investigation of the alleged facts	10
6.3 Motion for a resolution	10
6.4. Enforcement of the sanction	11
7. Protection of personal data	11
7.1. Information clause on personal data protection	11
7.2. Proportionality principle	12
7.3. Security and confidentiality measures	12
ANNEX I	14
Conduct that can be reported through the Whistleblower Channel	14
ANNEX II	18
Online platform for reporting complaints	18

1. Introduction to the Whistleblower Channel

The leading position and the prestige and reputation of the AZKOYEN Group are the result of many years of effort and hard work by each and every one of those who make up the company. However, the truth is that the inappropriate behaviour of a single employee can, at any time, damage its image and reputation. For this reason, the AZKOYEN Group works actively to prevent and avoid this possibility.

Thus, and among other issues, all employees and collaborators acting on behalf of and/or for the account of AZKOYEN are required to act in accordance with and respect at all times (i) current legislation, (ii) the Code of Conduct and (iii) internal policies and procedures. The cooperation of all employees in detecting possible irregular conduct is also of great importance in this preventive work.

In this regard, current legislation (*and especially the current Criminal Code, following its reform in 2010 and 2015, and Circular 1/2016 of 22 January of the State Attorney General's Office*) reinforces the need for companies to have "**criminal risk prevention models**", i.e. systems and control mechanisms that enable them to prevent, detect and react to the risk of a crime being committed in a company -and for its benefit- by any of its members.

And for the effectiveness of these prevention models, the so-called "Whistleblower Channel" plays a fundamental role, a channel which, in line with AZKOYEN's existing culture of ethics and compliance, allows its members to report possible risks and non-compliance.

Having said the above, this Policy will describe all the issues related to the operation of the AZKOYEN Whistleblowing Channel: who can make a complaint, against whom, in what situations and, above all, what steps will be followed when a complaint is received. All of this, of course, and as a fundamental pillar of the Channel, is subject to the strictest confidentiality.

In this way, everyone at Azkoyen will be aware of this tool, which is undoubtedly of great value and usefulness in preserving and protecting its image, prestige and reputation.

Subjective scope

The Whistleblower Channel is aimed at all the professionals (as set out below) of all the companies that make up AZKOYEN and external persons who have or may have knowledge of an irregularity committed by any other employee, manager or director.

2.1 Who should report through the Whistleblower Channel?

All (i) employees, (ii) managers (understood as those who provide management services for the company and hold powers of representation, organisation or control, regardless of whether their contractual relationship with

AZKOYEN is labour or commercial), (iii) members of its Board of Directors, as well as (iv) *its external collaborators (agents, subcontractors or other third parties acting under the authority of AZKOYEN)*, (v) all customers and suppliers of the Azkoyen Group, (vi) all customers and suppliers of the Azkoyen Group; must report, through the Whistleblowing Channel, any irregularity of which they are aware and which is included in their objective scope, without fear of being subject to dismissal or any other type of reprisal, and with the assurance that it will be treated with the utmost confidentiality.

The aforementioned typologies and/or categories shall hereinafter be referred to jointly and severally and for the exclusive purposes of this document as the "**Staff**".

In this respect, it is hereby stated for the record that by AZKOYEN Group we refer to the different trading companies that make up said Group, which are detailed on our web page <http://www.azkoyen.com/quienes-somos> and whose parent company is "GRUPO AZKOYEN, S.A." (for the purposes of this document we shall refer to all of them as the "**Group**").

2.2 Who can be reported through the Whistleblower Channel?

All employees, executives, members of the Board of Directors or external collaborators of the Group subject to its authority who have committed any irregularity or conduct within the objective scope detailed in this document may be the subject of a complaint.

3. Target Scope

The conduct that can be reported through the Channel (hereinafter "**the Target Scope**") is the conduct detailed in **Annex I** and listed below, which is criminalised under the Criminal Code (and other special laws) and may give rise to criminal liability for the Group:

- Public corruption
- Corruption in business
- Scam
- Punishable insolvencies
- Frustration at execution
- Computer damage
- Intellectual and industrial property offences
- Disclosure of business secrets
- Misleading advertising
- Money Laundering / Terrorist Financing
- Smuggling
- Offences involving risks caused by explosives and other agents
- Stock exchange offences
- Offence against the rights of foreign nationals
- Public health offences
- Pricing

- Offences against personal and family privacy
- Fraud against public finances
- Non-compliance with accounting obligations
- Social Security fraud
- Subsidy fraud/ Fraud against the general budgets of the EU
- Crimes against natural resources and the environment
- Fraudulent invoicing
- Counterfeiting of currency and stamped paper
- Price-fixing in public tenders and auctions
- Offences against workers' rights
- Refusal of inspection activity
- Hate Crimes

Likewise, any conduct that is contrary to the principles and rules of conduct established in the AZKOYEN Group Code of Conduct may also be reported through this Whistleblower Channel.

4. Means of receiving complaints How should you report?

In principle, and subject to certain exceptions listed below, all complaints should be submitted to the "Support Unit" of the Audit¹ Commission.

Complaints must be formulated and submitted via the digital platform, Complaints Channel, which complies with all legal precepts. Complaints may be nominative or anonymous, both cases being accepted by Azkoyen Group for subsequent investigation. The aforementioned channel can be accessed:

- Through the corporate website, in the following section or link: www.azkoyen.com/responsabilidad-social-corporativa/
- Through the employee portal, BeOne, at the following link: <https://beone.azkoyen.com/es/beone-home/>

Whistleblowers may remain anonymous or identify themselves when making the report, and all reports, both nominative and anonymous, will be accepted. In addition, throughout the entire procedure, the confidentiality of

¹ This Support Unit is the body to which the **Audit Committee** (*appointed by the Board of Directors to supervise the correct operation of AZKOYEN's Compliance model*) has delegated the function and responsibility of managing and investigating the complaints received.

At present, the Support Unit is made up of the Azkoyen Group's corporate director of Human Resources, who will also be able to count on expert legal advice for the different issues that may arise.

the identity of the complainant will be guaranteed, in compliance with the privacy requirements established by, among others, the Organic Law on Data Protection and the Spanish Data Protection Agency.

Privacy is one of the most important issues in the operation of the Channel. Precisely for this reason, all those persons - and external AZKOYEN professionals - who may intervene at any time in the event of a possible complaint, shall be subject to the most absolute obligation of confidentiality and professional secrecy.

5. Whistleblower protection measures

5.1 Prohibition of reprisals

Those persons who make any kind of complaint as provided herein and in good faith are protected against any kind of retaliation, discrimination, and penalisation on the grounds of the complaint they have made. AZKOYEN will sanction any type of retaliation against any Whistleblower in good faith, retaliation being understood as, among others and by way of example, possible dismissal, unjustified reduction of a possible bonus, transfer to another plant, or the assignment of lower-ranking duties and responsibilities.

A complainant who believes that reprisals have been taken against him or her solely as a result of having lodged a complaint may bring this to the attention of the Support Unit, which shall study the case and take appropriate measures to prevent or, failing this, to correct it.

The prohibition of retaliation provided for in the preceding paragraphs shall not prevent the adoption of appropriate disciplinary measures when the internal investigation establishes that the allegation is false and that the person who made the allegation was aware of its falsity, having acted in bad faith².

5.2 Confidentiality about the identity of the Whistleblower

AZKOYEN guarantees maximum confidentiality regarding the identity of the whistleblower.

As a measure to guarantee the said confidentiality, it is expressly stated that the exercise of the right of access by the reported party, provided for in the current Organic Law 15/1999, of 13 December, on the Protection of Personal Data, shall not entail access to the data relating to the identity of the reporting party (in the event that

² In this regard, it is also noted that, in accordance with the provisions of Article 456 et seq. of the Penal Code, accusation, false denunciation and simulation of crimes are considered crimes, punishable by a prison sentence of up to two years.

they have been provided). Consequently, and unless it is judicially determined, AZKOYEN shall not provide the identity of the complainant.

This principle of confidentiality is one of the basic pillars of the Whistleblowing Channel, the proper functioning of which depends on being able to guarantee whistleblowers that their identities will be protected, so as not to discourage whistleblowing.

Likewise, both the Support Unit and the Audit Committee are obliged to maintain professional secrecy regarding the identity of the whistleblower (anonymous whistleblowing is possible). If, exceptionally, any external advisor or other member of AZKOYEN were to participate in the investigation of the facts, he/she would be subject to the same obligation of confidentiality and professional secrecy.

5.3 Measures to deal with conflict of interest situations

In the event that the facts reported fall within the scope of the duties of the Support Unit, or of any of the members of the Audit Committee, or in any way may generate a conflict of interest for any of these persons, the person concerned shall refrain from intervening in the procedure for handling the complaints, as described below.

A conflict of interest shall be deemed to exist in those cases in which the private interests of any of these persons may limit their ability to carry out, with due objectivity, neutrality and impartiality, the processing and investigation of the complaints. This conflict is presumed to exist when the facts reported fall within the responsibilities and executive functions of any of the members of the Audit Committee or the Support Unit and may also exist when the facts affect any person with whom any of them has a family relationship (up to and including the third degree) or a business interest (holding shares or holdings in the same company in a percentage of more than 10%).

As a consequence of the foregoing, if the whistle-blower suspects that the facts may involve a conflict of interest with the Support Unit, he/she may file the complaint directly with the Audit Committee; or with the secretary of the Board of Directors if the conflict of interest affects any of the members of the Audit Committee. In such cases, and provided that the existence of such conflict of interest is verified, an external expert shall be entrusted with the processing and investigation of the complaint, and the budgetary management controls that may be applicable shall not have to be followed for the hiring thereof.

6. Procedure for handling complaints

6.1 Receipt of complaints

With the exception of the cases provided for in section 5.3. above, all complaints made will be made on the online platform and investigated by the Support Unit, which will be responsible for receiving them, carrying out a preliminary analysis of the facts reported and their suitability for the form provided. The Support Unit will then decide whether to initiate the corresponding investigation or whether to reject the complaint, as provided for in this Policy, with a maximum period of five (7) days from receipt to confirm receipt of the complaint to the complainant and the start of the investigation. The subsequent process would be as follows:

- a) **Inadmissibility of the complaint:** if the complaint does not comply with the formal requirements established herein, or if it is evident that the facts reported do not constitute an infringement within the objective scope of the Complaints Channel, the Support Unit shall reject the complaint.

Following this, and within a non-extendable period of two (2) working days, the Support Unit shall notify the Audit Committee of its decision, which, if there are reasons to justify it and exceptionally, may annul such decision and request it to proceed to admit it for processing. The Committee shall have a period of ten (10) working days from receipt by its secretary of the Support Unit's decision to do so.

- b) **Admission of the complaint for processing and initiation of the investigation phase:** when the complaint complies with the formal requirements and, in addition, the facts reported fall within the objective scope of the Complaints Channel, and there are indications that they have taken place, the Support Unit will agree to admit it for processing.

After following the above milestones and deadlines, the decision taken by the Support Unit at this stage of the procedure shall be communicated to the complainant within a maximum of ten (10) working days, unless a longer period is necessary for justified reasons.

Likewise, any person who has been the subject of a complaint admitted for processing will be informed of **(i)** the receipt of the complaint, **(ii)** the fact of which he/she is accused, **(iii)** the departments and third parties who, where appropriate, may be recipients of the complaint and **(iv)** how to exercise his/her rights of access, rectification, cancellation, and opposition, in accordance with data protection regulations.

However, the data subject's right of access shall be limited to his or her own personal data processed, which is why, given the confidential nature of the complaints, the data subject may not exercise this right to know the identity and personal data of the complainant.

Exceptionally, if the Support Unit considers that there is a risk that notifying the reported person may jeopardise the investigation, such notification may be postponed until the risk disappears. In any case, the period for informing the accused shall not exceed one (1) month from receipt of the complaint, with the possibility of extending this period to a maximum of three (3) months if there are justified reasons for doing so. This is without prejudice to the fact that the law may expressly and bindingly establish different deadlines, in which case these shall be the ones to be observed.

6.2 Investigation of the alleged facts

Once the complaint has been accepted for processing, the Support Unit shall initiate the appropriate investigations to verify the veracity of the facts reported. To this end, it may request any information and documentation it deems necessary to try to clarify the facts reported.

For their part, and whenever requested to do so, AZKOYEN personnel must cooperate fully with the investigation work carried out.

In the event that, due to the nature of the facts, it is considered that the investigation will be complex, the assistance or specialised advice of an external expert may be sought, which will be coordinated with the Support Unit and the Audit Committee.

6.3 Motion for a resolution

Once the investigation has been completed, two proceedings will be carried out:

- In the first instance, the Support Unit shall report to the Audit Committee on the results achieved and shall either (i) propose to close the complaint or (ii) formulate a proposal for a resolution.
- Having done so, and in the light of this report, the Audit Committee shall adopt such decision as, in its opinion, may be appropriate.

In this regard, the Audit Committee shall agree to close the complaint and the proceedings carried out when the facts reported have not been sufficiently accredited, or when they do not constitute an infringement included in the objective scope of the Whistleblowing Channel.

On the other hand, if the Audit Committee considers that the facts reported have been sufficiently accredited and, furthermore, constitute an infringement included in the objective scope of the Whistle-blowing Channel, it shall issue a reasoned resolution indicating the legal measures, of whatever nature, to be adopted. When issuing this decision, the Audit Committee shall not be bound by the proposal made by the Support Unit but shall have full freedom and sovereignty to decide what it deems most appropriate in each case.

At any point in the procedure, the Audit Committee may also rely on legal advice and assistance from an external subcontracted expert, for example, to advise it on aspects such as the wording of the facts, their classification, or the adoption of the most appropriate disciplinary measures in each case.

In the event of a conflict of interest, as described in section 5.3. above, the final decision shall be taken jointly by the Chairman and the Secretary of the Board of Directors.

6.4. Enforcement of the sanction

The sanction or disciplinary measures agreed in each case shall be applied by the person or persons who have been attributed these functions, under sufficient authority.

In the case of employment-related sanctions, the person in charge shall be the Human Resources Director. If the sanction is of a commercial nature (contractual termination, etc.) or requires the exercise of legal action, it shall be adopted by the Audit Committee and executed by a person with sufficient power of attorney.

7. Protection of personal data

When designing this Channel, AZKOYEN fully complies with the applicable regulations on data protection; especially Organic Law 15/1999, of 13 December, on the Protection of Personal Data ("LOPD") and its implementing regulations. Likewise, the Whistleblowing Channel has been designed in accordance with Legal Report 0128/2007 of the Spanish Data Protection Agency "Creation of internal whistleblowing systems in companies (*whistleblowing* mechanisms)", and with the "Report 1/2006 on the application of European Union data protection rules to internal *whistleblowing* mechanisms in the field of accounting and internal audit controls, the fight against fraud and banking and financial crime", of the Article 29 Working Group of the European Commission.

7.1. Personal data protection information clause

The personal data collected within the framework of the Complaints Channel will be processed for the sole purpose of processing the complaints received and, if appropriate, investigating the reality of the facts reported, thus complying with the legal requirement established in Organic Law 1/2015, of 30 March and in Organic Law 15/1999, of 13 December on the Protection of Personal Data.

The data collected within the framework of a complaint, and which give rise to the opening of the corresponding investigation will be included in the "Complaints Channel" file, duly declared to the Spanish Data Protection Agency. The party responsible for said file is GRUPO AZKOYEN, S.A. with C.I.F. A31065618 and registered office at Avda. San Silvestre, s/n, 31.350 Peralta - Navarra - (Spain).

On the other hand, it is expressly stated that the data contained in those complaints that are not admitted for processing will not be included in any file and will be deleted immediately.

Both the complainant and the respondent will be duly informed, in each case, of the specific persons and bodies to whom their data will be disclosed, in accordance with the provisions of this policy, especially as regards the possible non-communication of the identity of the complainant to the respondent.

To revoke the consents granted, as well as to exercise the rights of access, rectification, cancellation, opposition, limitation, portability, and the right not to be subject to automated decisions, you may send a written request to the following postal address: Avenida San Silvestre, s/n. C.P. 31350 Peralta (Navarra-Spain) or by e-mail to the following address: responsableseguridad@azkoyen.com

The request must include name and surname(s) of the interested party; copy of the National Identity Document, passport or other valid identification document of the interested party and, if applicable, of his/her representative, as well as proof of representation; address for notification purposes and specification of the purpose of the request.

Notwithstanding the above, the data subject's right of access will be limited to his or her own personal data, with no access to the data on the identity of the complainant (in the event that the complainant has identified himself or herself in the complaint) - given the confidential nature of the Complaints Channel.

7.2. Proportionality principle

Personal data collected in the framework of the Whistleblowing Channel:

- ✓ shall be limited to those strictly and objectively necessary to deal with the complaints and, where appropriate, to verify the reality of the facts complained of;
- ✓ will at all times be processed in accordance with the applicable data protection rules, for legitimate and specific purposes in connection with the investigation that may arise as a result of the complaint;
- ✓ shall not be used for incompatible purposes;
- ✓ shall be adequate and not excessive in relation to the above-mentioned purposes.
- ✓ It provides for the possibility for the complainant to choose to remain anonymous.

7.3. Security and confidentiality measures

AZKOYEN shall ensure that all the necessary technical and organisational measures are adopted to preserve the security of the data collected in order to protect them from unauthorised disclosure or access.

To this end, AZKOYEN has adopted appropriate measures to guarantee the confidentiality of all data and will ensure that the data relating to the identity of the complainant (if any) are not disclosed to the person reported during the investigation, respecting in all cases the fundamental rights of the person, without prejudice to any actions that may be taken by the competent judicial authorities, as the case may be.

ANNEX I

Conduct that can be reported through the Whistleblower Channel

The conduct that can be reported through the AZKOYEN Group's Whistleblower Channel includes any **breach of the principles and rules of conduct set out in its Code of Conduct**, which is available to all Group professionals on the Employee Portal.

Likewise, the conduct defined in the Criminal Code and the offences provided for in other special laws, which may give rise to criminal liability for the Group, such as the following, shall also be reportable:

- ✓ **Bribery:** Offering or giving officials, authorities, organisations and public administrations a gift or compensation, financial or otherwise, with the intention of obtaining a benefit for AZKOYEN, whether lawful or unlawful.
- ✓ **Influence peddling:** Likewise influencing, taking advantage of any situation derived from a personal relationship, to achieve a resolution that may directly or indirectly generate an economic benefit for AZKOYEN.
- ✓ **Corruption in business dealings:** That a director, administrator, employee or collaborator of AZKOYEN, either personally or through an intermediary, receives, requests or accepts an unjustified benefit or advantage of any nature, for himself or for a third party, as consideration for unduly favouring another in the acquisition or sale of goods, or in the contracting of services or in business relations. Conversely, the promise or giving of a benefit to a third party for the acquisition or sale of goods in commercial relations.
- ✓ **Corruption in international transactions:** Offering or giving an undue advantage or benefit to public officials to obtain favourable treatment in the conduct of international business.
- ✓ **Fraud:** Deceiving another person, for profit, in order for him to carry out an act of disposition that is detrimental to himself or to a third party.
- ✓ **Misleading advertising:** Making offers or advertising of products or services, where false allegations are made or uncertain characteristics are stated about them, in such a way as to cause serious and manifest prejudice to consumers.
- ✓ **Discovery and disclosure of trade secrets:** Taking possession by any means of data, documents, whether written or electronic, computer media or other objects constituting confidential information of another company, entity, etc., for their use, dissemination, disclosure, or transfer.

- ✓ **Subsidy fraud:** Obtaining subsidies or aid from the Public Administrations in an amount or for a value of more than 120,000 euros by falsifying the conditions required for their concession and concealing those that would have prevented it.
- ✓ **Fraud against the Public Treasury:** Defrauding the Public Treasury (state, regional, provincial, or local) of more than 120,000 euros; evading the payment of taxes, amounts withheld or that should have been withheld or payments on account of remuneration in kind, unduly obtaining refunds or enjoying tax benefits in the same way.
- ✓ **Social Security fraud:** Avoiding the payment of Social Security contributions by unduly obtaining refunds or taking advantage of deductions inappropriately.
- ✓ **Breach and falsification of accounting obligations:** Serious breach of the obligation to keep business accounts and accounting books and/or records. It represents a type of offence that is often combined with other fraudulent conducts, as these are often carried out by means of double bookkeeping and false accounting entries.
- ✓ **Offences against natural resources and the environment:** Directly or indirectly causing or carrying out emissions, discharges, radiations, extractions, excavations, landings, groundings, noises, vibrations, injections, or deposits, in the atmosphere, soil, subsoil or terrestrial, subterranean or maritime waters; establishing deposits or dumps of solid or liquid waste or residues that are toxic or dangerous and may seriously damage the balance of natural systems or the health of people.
- ✓ **Frustration of enforcement:** Carrying out any act of disposal of assets or generating obligations that hinders or prevents a seizure or a procedure for claiming an amount from being carried out. Concealing assets in judicial or administrative enforcement proceedings. Making unauthorised use of assets seized by the authorities without the authorisation of the depository.
- ✓ **Punishable insolvencies:** In the event that the company is in insolvency proceedings, this offence would occur when an act of disposal of assets is carried out to unduly reduce the assets that are a guarantee for the fulfilment of obligations, or to make it difficult or impossible for the creditor to know the debtor's true economic situation.
- ✓ **Offences against Intellectual Property:** Reproduce, plagiarise, or communicate publicly, in whole or in part, a literary (book), artistic (painting or photograph) or scientific (specific theory, applications or computer programmes) work, or its transformation, interpretation or artistic execution fixed on any type of support or communicated by any means, without the authorisation of the owners. For example, this offence is applicable in cases where computer applications or software are used without the corresponding licence for use.




- ✓ **Industrial Property Offences:** Reproducing, imitating, etc. a distinctive sign without the consent of the owner, so as to obtain another sign identical or confusingly similar to it, to distinguish the same or similar goods, services, activities, or establishments.
- ✓ **Computer damage:** Deleting, damaging, deteriorating, deleting, or making inaccessible, data, computer programmes or electronic documents of others, without authorisation and when the result produced would be serious. Impeding or hindering the operation of other people's computer systems.
- ✓ **Counterfeiting currency and stamped effects:** Altering or manufacturing counterfeit currency. Bringing into the country or exporting counterfeit or altered currency. Transporting, selling or distributing counterfeit or altered currency with knowledge of its counterfeit nature.
- ✓ **Offences against personal and family privacy:** Taking, using or modifying, without authorisation and to the detriment of a third party, reserved personal or family data of another person that is recorded in computer, electronic or telematic files or media or in any other public or private file or register. Unlawfully accessing a computer system in order to take possession of personal data contained therein.
- ✓ **Against the rights of foreign nationals:** Promoting, encouraging or facilitating illegal trafficking or illegal immigration.
- ✓ **Money laundering:** Accepting funds, deposits, etc. originating from the commission of an offence, or performing any other act to conceal such illicit origin, or to assist the person who has participated in the offence. It can be committed recklessly if it is done without due diligence, i.e. it is not necessary for the perpetrator to want and know that the offence is going to be committed.
- ✓ **Terrorist financing:** Providing, collecting or accepting funds with the intention that they be used to commit crimes related to terrorist organisations and groups.
- ✓ **Offence against public health:** Offering on the market products that are harmful to health, and/or that do not comply with the expiry date or composition requirements established by law or regulation. Also manufacturing substances harmful to health, dispensing, supplying or trading in them.
- ✓ **Against workers' rights:** Putting the life, health and safety of workers at serious risk due to the infringement of occupational risk prevention regulations. This offence can be committed recklessly. Using deception or abuse of a situation of necessity to impose working or Social Security conditions on workers that prejudice, suppress or restrict their rights. Imposing inadequate working conditions or conditions contrary to occupational health and safety; treating workers in conditions of inequality and discrimination; preventing or limiting the right to freedom of association.

- ✓ **Stock exchange offence:** Using or supplying any information relevant to the quotation of any kind of financial instrument. Disseminating news or rumours about persons or companies, knowing them to be false, with the aim of altering or preserving the price of the quotation of a security or financial instrument. Misrepresenting the economic-financial information contained in the issue prospectuses of any financial instruments.
- ✓ **Handling of toxic, corrosive and other substances:** Contravening established safety standards in the manufacture, handling, transport, possession or marketing of explosives, flammable or corrosive, toxic and asphyxiating substances, endangering the life, physical integrity or health of people or the environment.
- ✓ **Refusal to cooperate with the inspection authorities in the case of companies subject to or operating in markets subject to administrative supervision.**
- ✓ **Illegal financing of political parties:** Giving donations or contributions to a political party, federation, coalition or grouping of voters in an illegal manner.
- ✓ **Fraudulent invoicing:** Altering or manipulating the automatic devices that measure the cost of the products sold or services offered (meters, taximeters, etc.) with the aim of invoicing higher amounts, causing damage to the consumer.
- ✓ **Smuggling:** Importing or exporting lawfully traded goods in an irregular manner, provided that the value of the goods, merchandise, goods or effects is equal to or greater than 150,000 euros. Failing to comply with customs regulations in any other way.
- ✓ **Price-fixing in public tenders and auctions:** Soliciting any benefit in order not to take part in a public tender or auction, attempting to drive bidders away by means of threats, gifts, promises or any other artifice, concerting with another bidder with the aim of altering the auction price, or fraudulently abandoning an auction after having been awarded the contract.
- ✓ **Price fixing:** Altering the prices that would result from the free competition of products or services.

ANNEX II

Online platform for reporting complaints

[Home](#) [Privacy policy](#) [Secure Inbox](#) [English](#)

Make a report  

What is your suspicion? ***Required**

Do you work in the organisation?

Choose an option ▼

In which company did the incident take place? ***Required**

Please give the name of the affected department:

Who is involved in the incident?

In which country did the incident take place?

In which city did the incident occur?

When did the incident take place?

Contact information

You can choose to submit the report anonymously, but we encourage you to provide your name and contact details in the fields below.

Stay anonymous

Stay anonymous

Name

Phone number

Email

Secure Inbox

You must create a secure Inbox even if you have already provided your contact information. This makes it safer and easier for us to communicate.

Use the Inbox if you want to send more information about the case or answer potential questions.

If you have already created an Inbox on this device, use that password to add this case to your secure Inbox.

In order to follow up on the case, please log in with your password.

Once your case has been processed, you can find the answer to your request in the Inbox. If you have provided your email address, you will receive an automatic notification once a message has been added.

Enter your password

The password must:

- Have a minimum length of 8 characters.
- Must contain at least one lower case and one capital letter.
- Contain at least one digit.

Password

Repeat password

I have read and understand the Privacy Policy and accept the terms and conditions.

[Click here to read the privacy policy](#)